UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,600	07/26/2001	Chris A. Barton	NAI1P020/01.139.01	8707

28875 7590 03/22/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/916,600	BARTON, CHRIS A	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-7,10-18,20-23 and 26-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1,2,4-7,10-18,20-23 and 26-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02152005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-43 have been considered.

Information Disclosure Statement

The information disclosure statement filed 2/15/05 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because the references are not listed on a 1449 Form. The references have been submitted on an 892 Form. For the examiner to consider patents in an IDS, they need to be listed on a 1449 Form.

It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609 ¶ C(1).

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 42 is rejected under 35 U.S.C. 112, first paragraph as providing new matter not originally described in the Specification. No where in the Specification does the applicant describe that it is determined whether the storage is disabled "only after" determining whether the scanning module is disabled. Embodiments, such as Figs 4 and 5, reveal that the storage is checked to see it if is disabled after the scanning module is checked to see if it is disabled but the Specification does not reveal that the check must occur this way. Accordingly, the claim has been rejected as describing new matter.

Appropriate correction is required.

Claim 43 is rejected as dependent on claim 42.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700.

As per claims 1 and 17, the applicant describes a method for scanning data read from storage comprising the following limitations which are met by Makita in view of Flint:

a) receiving a request for data saved in storage from a central processing unit (Makita: [0180]);

b) scanning the requested data for malicious code (Makita: [0182]);

c) transmitting the data from the storage to the central processing unit if malicious code is not found in the data during scanning (Makita: [0184]);

d) wherein the scanning is performed by a scanning module coupled to a storage subsystem controller (Makita: [0091] and Fig 15);

e) wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module (Flint: Col 9, lines 5-24).

The applicant has incorporated original claim 3 into part d) above and original claims 8 and 9 into part e). Makita describes all the limitations of parts a) through d) above. As per part d), the storage subsystem controller is the file management unit (211 of Fig 15) which is coupled to the virus scan unit (413) of Fig 15. The central processing unit pertains to the CPU on the host computer (110 of Fig 15).

Makita does not describe disabling the scanning module. Makita does describe, as discussed in the first office action, that other functions such as formatting can be enabled or disabled by the user (Makita: [0057] and [0058]). However, Makita never discloses that the scanning module can be enabled or disabled by the user.

Flint discloses a similar virus scanning system in which the user can enable or disable the scanning module at will. Being able to enable or disable the scanning module is an obvious improvement because it allows for data to be transmitted efficiently without a scan when the user is sure that data is virus-free or when the user does not care to invest the time to make sure that data is virus free. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Flint with those of Makita and make the virus scanner capable of being disabled or enabled by the user for the case of efficiency when the scanner is not needed.

As per claims 2 and 18, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage is selected from the group consisting of a hard drive, a compact disc-read only memory (CD-ROM), and a floppy disc (Makita: [0004], [0015], and Fig 4);

As can be seen in the paragraphs and figure referenced above, the storage of Makita is a hard drive.

As per claims 4,20, and 38, the applicant describes the method of claims 1,17, and 35, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage subsystem controller is coupled to a storage driver which is coupled to the central processing unit, where the storage driver is coupled between the storage subsystem controller and the central processing unit, so that the storage subsystem controller and the central processing unit must communicate therethrough (Makita: Fig 15 and [0010]);

According to the applicant's specification, the storage driver "interfaces with the operating system running on the cpu for communicating read and write requests to the storage subsystem controller" (applicant: page 8). The storage driver is the interface unit (21 of Fig 15), the storage subsystem controller is the file management unit (211 of Fig 15), and the CPU is the CPU on the host computer (110 of Fig 15). All of these components are coupled together as illustrated in Fig 15.

As per claims 5 and 21, the applicant describes the method of claims 3 and 19, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage subsystem controller is coupled to the storage (Makita: Fig 15);

The applicant should note as described above, the storage subsystem controller is the file management unit (211 of Fig 15).

As per claims 6-7 and 22-23, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning module includes software (Makita: [0213] and Fig 15);

The primary reference discloses a scanning module unit which incorporates both software and hardware components. Regarding the software component, the primary reference discloses that the virus check can take the form of a program [0213]. Regarding the hardware component, the primary reference discloses the use of a segregated virus check unit which is connected to a plurality of other units, such as a storage unit (22 of Fig 15) and an interface unit (21 of Fig 15) in a bus-style system.

As per claims 10 and 26, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Further comprising executing an event based on results of the scanning [0183];

Two events are mentioned: halting the scanning/transmission of data process and alerting the user.

As per claims 11 and 27, the applicant describes the method of claims 10 and 26, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the event includes an alert (Makita: [0183]).

As per claims 12 and 28, the applicant describes the method of claims 10 and 26, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Further comprising disabling the scanning module in response to the event (Makita: [0183]);

The applicant should note that the scanning/transmission of data process is halted.

As per claims 13 and 29, the applicant describes the method of claims 12 and 28, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein data is precluded from being transmitted from the storage to the central processing unit upon disabling of the scanning module (Makita: [0183]);

As per claims 14 and 30, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning includes content scanning (Makita: [0054] and [0055]);

The applicant should note that the primary reference includes the use of content scanning, which is used to determine a format of data and format the data to a user-selected format, and virus scanning, which is used to detect malicious data.

As per claims 15 and 31, the applicant describes the method of claims 1 and 17, which are anticipated by Makita in view of Flint (see above), with the following limitation which is also anticipated by Makita:

Wherein the scanning includes virus scanning (Makita: [0182]);

As per claims 16 and 32, the applicant describes the method of claims 1 and 17, which are anticipated by Makita (see above), with the following limitation which is also anticipated by Makita:

Wherein the storage is accessible via a network (Makita: [0036] and [0196] and Fig 19);

As described by the applicant, the system takes place in "an environment in which the storage device is connected to and/or disconnected from each of a plurality of host computers" [0036].

As per claims 33 and 34, the applicant describes a method for scanning data written to storage comprising the following limitations which are met by Makita in view of Flint:

a) receiving a request for data to be written in storage, the request being received from a central processing unit (Makita: [0174]);

b) scanning the data for malicious code (Makita: [0174]);

c) writing the data to the storage if malicious code is not found in the data during the scanning (Makita: [0177]);

d) wherein the scanning is performed by a scanning module coupled to a storage subsystem controller (Makita: [0091] and Fig 15);

e) wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the scanning module (Flint: Col 9, lines 5-24);

For motivation for combining the ideas of Makita with those of Flint, see the rejection for claim 1.

As per claims 35 and 39, the applicant describes a system for scanning data read from storage comprising the following limitations which are met by Makita in view of Flint:

a) storage for saving data therein (Makita: 22 of Fig 15);

b) a storage subsystem controller coupled to the storage for controlling access to the data saved therein (Makita: 211 of Fig 15);

c) a central processing unit coupled to the storage subsystem controller for issuing read requests for reading the data saved therein for processing purposes, and write requests for writing data to the storage (Makita: 110 of Fig 15; 14 of Fig 4; [0008]);

d) a scanning module coupled to the central processing unit and the storage subsystem controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests (Makita: 413 of Fig 15);

e) an event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning (Makita: 211 of Fig 15; [0183]; [0091]);

f) wherein the central processing units is conditionally allowed to read the data saved in the storage and write data to the storage based on the results of the scanning (Makita: [0183] and [0184]);

g) wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted between the storage and the central processing unit upon the disabling of the scanning module (Flint Col 9, lines 5-24);

As described earlier by the examiner, regarding the use of a central processing unit, the primary reference discloses an operating system control unit. The operating system control unit embodies the CPU as it is well known in the art that an operating system runs on the central processing unit. The role of the operating system control unit of the primary reference is identical to the role of the CPU as described in the applicant's invention. The operating system control unit controls the read and write requests which take place between the host computer and the remote storage ([0008] and Fig 4).

According to the applicant, the central processing unit issues read and write requests between the computer and the storage (Page 5).

Regarding part e), the file management unit acts as the event manager module in addition to acting as the storage subsystem controller. The file management unit controls the transmission between the storage and the host computer [0091]. When a virus is detected, transmission between the remote storage and the host computer is halted [0183]. Since the file management unit executes the security event of halting the transmission between the storage and the host computer, the file management unit acts as the event manager module.

For motivation for combining the ideas of Flint with those of Makita see the rejection for claim 1.

As per claim 36, the applicant limits the system of claim 35, which is anticipated by Makita in view of Flint (see above), with the following limitation which is also met by Makita:

Wherein the scanning module is coupled to the storage subsystem controller via a bus (Makita: Fig 15);

Makita discloses a connection between the scanning module, or virus check unit (413 of Fig 15), and the storage subsystem controller, or file management unit (211 of Fig 15) in a bus configuration where data is transferred between the segregated units.

As per claim 37, the applicant limits the system of claim 35, which is anticipated by Makita in view of Flint (see above), with the following limitation which is also met by Makita:

Wherein the scanning module is directly coupled to the storage subsystem controller (Makita: Fig 15).

The scanning module is 413 of Fig 15 and the storage subsystem controller is 211 of Fig 15.

As per claim 40, the applicant describes the method of claim 1, which is met by Makita in view of Flint (see above), with the following limitation which is also met by Flint:

Wherein the user includes a remote administrator (Flint: Col 2, lines 19-20);

Flint discloses the idea that a user can be an administrator.

Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Makita in view of Flint in further view of Browne, U.S. Patent No. 6,272,533.

As per claim 41, the applicant describes the method of claim 1, which is met by Makita in view of Flint (see above), with the following limitation which is met by Browne:

Wherein the user is allowed to disable the storage, and the data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage (Browne: Col 4, lines 61-64);

Makita in view of Flint discloses all the limitations of independent claim 1. However, Makita in view of Flint fail to disclose any method for preventing data to be transmitted from storage by a user.

Browne discloses a secure computing system in which a manual switch (which is operating by a user) can be pressed so that data is precluded from being written to a storage device. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Browne with those of Makita in view of Flint and add a manual switch to prevent the writing of data to a storage location for security reasons in the event that a user may not want the CPU to write data to the storage device.

Response to Arguments

Applicant's arguments, see Remarks, filed 1/28/05, with respect to the rejection(s)of claim(s) 8 and 9 under Makita have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Flint, U.S. Patent No. 6,735,700.

Applicant's arguments with respect to the rejection(s)of claim 4 have been fully considered but they are not persuasive. Fig 15 of Makita clearly shows the limitations of claim 4. Furthermore, the

applicant has provided no argument to rebut the examiner's original rejection, so the examiner does not understand the applicant's argument.

Applicant's arguments with respect to the rejection(s)of claim 12 have been fully considered but they are not persuasive. Makita's system involves a scanning/transmission process in which data is scanned for transmission to the CPU. As disclosed by Makita, this process is stopped [0183] in response to detection of a virus.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

***